PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-247022
(43)Date of publication of application : 30.08.2002

(51)Int.Cl. H04L 9/08
H04H 1/00

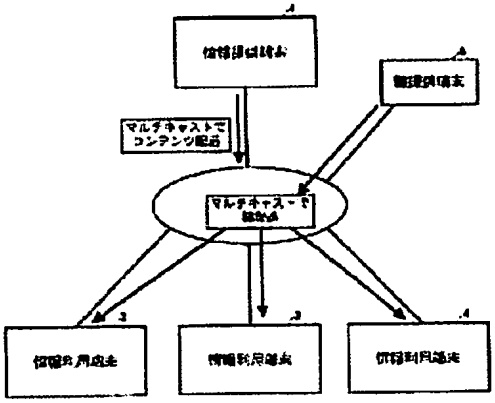
(21)Application number : 2001-046708
(22)Date of filing : 22.02.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : IORI SACHIKO
MIYAKE NOBUHISA
NAKAZATO KANA

(54) METHOD FOR DELIVERING INFORMATION, METHOD FOR UTILIZING INFORMATION, THEIR EXECUTION DEVICE AND PROCESSING PROGRAM, AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide technology capable of efficiently delivering a key for deciphering ciphered contents to plural information using terminals.
SOLUTION: The information delivering method for delivering contents from an information providing terminal to plural information using terminals by a multicast state is provided with a step for generating a key for ciphering or deciphering contents, a step for generating ciphered key data obtained by ciphering the key, a step for delivering the generated ciphered key data to respective information using terminals by the multicast state, a step for ciphering the contents by the generated key, and a step for delivering the ciphered contents to respective information using terminals by the multicast state.

図1



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－247022
（P2002－247022A）
(43)公開日　平成14年８月30日(2002.8.30)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｈ　1/00	Ｆ	５Ｊ１０４
Ｈ０４Ｈ　1/00		Ｈ０４Ｌ　9/00	６０１Ｂ	
			６０１Ａ	

審査請求　未請求　請求項の数19　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－46708(P2001－46708)

(22)出願日　平成13年２月22日(2001.2.22)

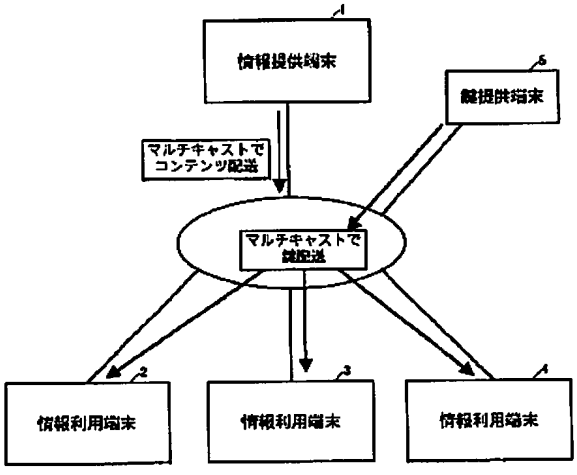
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　庵　祥子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　三宅　延久
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　情報配送方法、情報利用方法及びその実施装置並びにその処理プログラムと記録媒体

(57)【要約】
【課題】　暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能な技術を提供する。
【解決手段】　コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送方法において、コンテンツを暗号化または復号化する為の鍵を生成するステップと、前記鍵を暗号化して暗号化鍵データを生成するステップと、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送するステップと、前記生成した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップとを有するものである。

図１



【特許請求の範囲】
【請求項１】　コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送方法において、
コンテンツを暗号化または復号化する為の鍵を生成するステップと、前記鍵を暗号化して暗号化鍵データを生成するステップと、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送するステップと、
前記生成した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップとを有することを特徴とする情報配送方法。
【請求項２】　暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送するステップと、変更後の鍵の再配送要求を情報利用端末から受付けるステップと、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送するステップとを有することを特徴とする請求項１に記載された情報配送方法。
【請求項３】　暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の２つ以上のデータを同一のマルチキャストで各情報利用端末に配送することを特徴とする請求項１または請求項２のいずれかに記載された情報配送方法。
【請求項４】　マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用方法において、
利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データをマルチキャストで取得するステップと、前記取得した暗号化鍵データを保存するステップと、
暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するステップと、前記保存した暗号化鍵データを復号化して鍵を生成するステップと、前記取得した暗号化コンテンツを前記生成した鍵で復号化するステップと、前記復号化したコンテンツを再生するステップとを有することを特徴とする情報利用方法。
【請求項５】　暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得するステップと、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認するステップと、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求するステップと、前記再配送を要求した変更後の暗号化鍵データを取得するステップとを有することを特徴とする請求項４に記載された情報利用方法。
【請求項６】　暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の２つ以上のデータを同一のマルチキャストにより取得することを特徴とする請求項４または請求項５のいずれかに記載された情報利用方法。
【請求項７】　コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末において、
コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記鍵を暗号化して暗号化鍵データを生成する鍵暗号化部と、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送する鍵配送部とを備えることを特徴とする鍵提供端末。
【請求項８】　暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送する鍵変更予告配送部と、変更後の鍵の再配送要求を情報利用端末から受付ける鍵再配送受付部と、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送する鍵再配送部とを備えることを特徴とする請求項７に記載された鍵提供端末。
【請求項９】　マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末において、
利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データをマルチキャストで取得する鍵取得部と、前記取得した暗号化鍵データを保存する鍵保存部と、
暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記保存した暗号化鍵データを復号化して鍵を生成する鍵復号化部と、前記取得した暗号化コンテンツを前記生成した鍵で復号化するコンテンツ復号化部と、前記復号化したコンテンツを再生するコンテンツ再生部とを備えることを特徴とする情報利用端末。
【請求項１０】　暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得する鍵変更予告取得部と、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認する鍵確認部と、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求する鍵再配送要求部と、前記再配送を要求した変更後の暗号化鍵データを取得する鍵再取得部とを備えることを特徴とする請求項９に記載された情報利用端末。
【請求項１１】　暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の２つ以上のデータを同一のマルチキャストにより取得することを特徴とする請求項９または請求項１０のいずれかに記載された情報利用端末。
【請求項１２】　コンテンツをマルチキャストで情報利用端末に提供する情報提供端末において、
利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末から取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、
前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化

コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の２つ以上のデータを同一のマルチキャストで各情報利用端末に配送するコンテンツ配送部とを備えることを特徴とする情報提供端末。

【請求項１３】　コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末としてコンピュータを機能させる為のプログラムにおいて、

コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記鍵を暗号化して暗号化鍵データを生成する鍵暗号化部と、前記生成した暗号化鍵データをマルチキャストで各情報利用端末に配送する鍵配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項１４】　暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送する鍵変更予告配送部と、変更後の鍵の再配送要求を情報利用端末から受付ける鍵再配送受付部と、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送する鍵再配送部としてコンピュータを機能させることを特徴とする請求項１３に記載されたプログラム。

【請求項１５】　マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末としてコンピュータを機能させる為のプログラムにおいて、

利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データをマルチキャストで取得する鍵取得部と、前記取得した暗号化鍵データを保存する鍵保存部と、

暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記保存した暗号化鍵データを復号化して鍵を生成する鍵復号化部と、前記取得した暗号化コンテンツを前記生成した鍵で復号化するコンテンツ復号化部と、前記復号化したコンテンツを再生するコンテンツ再生部としてコンピュータを機能させることを特徴とするプログラム。

【請求項１６】　暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得する鍵変更予告取得部と、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認する鍵確認部と、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求する鍵再配送要求部と、前記再配送を要求した変更後の暗号化鍵データを取得する鍵再取得部としてコンピュータを機能させることを特徴とする請求項１５に記載されたプログラム。

【請求項１７】　暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の２つ以上のデータを同一のマルチキャストにより取得することを特徴とする請求項１５または請求項１６のいずれかに記載されたプログラム。

【請求項１８】　コンテンツをマルチキャストで情報利用端末に提供する情報提供端末としてコンピュータを機能させる為のプログラムにおいて、

利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末から取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、

前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツ、暗号化コンテンツの鍵を暗号化した暗号化鍵データまたは暗号化コンテンツの鍵が変更されることを予告する鍵変更予告の内の２つ以上のデータを同一のマルチキャストで各情報利用端末に配送するコンテンツ配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項１９】　請求項１３乃至請求項１８のいずれか１項に記載されたプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンテンツをマルチキャストで配送する情報配送システムに関し、特にストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送された復号鍵で復号化することにより情報の利用制御を可能とする情報配送システムに適用して有効な技術に関するものである。

【０００２】

【従来の技術】従来、複数の利用者に対してストリームコンテンツ等の同一のコンテンツを提供する場合、マルチキャストを用いることにより効率良くコンテンツの配送を行うことができる。このマルチキャストを用いたコンテンツの配送では、利用者がマルチキャストアドレスを指定することにより、誰でも簡単にそのコンテンツを利用することができる。

【０００３】また前記マルチキャストを用いて、利用資格を有する特定の利用者向けにコンテンツを提供しようとする場合には、そのコンテンツを利用者のみが復号できる状態で（例えば利用者に予め配られている鍵を利用する等）暗号化し、その暗号化コンテンツをマルチキャストで配送するという手法がある。利用者は、マルチキャストアドレスを指定して受信した暗号化コンテンツを、予め配られている鍵で復号化することにより、そのコンテンツを利用することができる。

【０００４】

【発明が解決しようとする課題】前記従来技術でマルチキャストを用いて暗号化すること無くコンテンツの配送を行った場合、マルチキャストアドレスを指定すれば誰でも簡単にそのストリームコンテンツを利用できる為、利用資格を有する特定の利用者向けにコンテンツを提供しようとした場合、前記暗号化を用いないマルチキャス

トではコンテンツの不正利用が行われるという問題があった。

【０００５】またストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送した場合、盗聴によるストリームコンテンツの不正利用は防御しているが、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能な為、不正利用される恐れがあるという問題があった。

【０００６】更に、暗号化コンテンツを復号化する為の鍵が、通信パケットの欠落や通信の遅延で送付されなかった場合、正当な利用者であってもストリームコンテンツを利用できない可能性があるという問題があった。

【０００７】本発明の目的は上記問題を解決し、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能な技術を提供することにある。

【０００８】本発明の他の目的は暗号化コンテンツを復号化する為の鍵の配送をより確実に行うことが可能な技術を提供することにある。

【０００９】

【課題を解決するための手段】本発明は、コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送システムにおいて、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するものである。

【００１０】本発明の情報配送システムでは、コンテンツを暗号化または復号化する為の鍵を生成した後に、その鍵を各情報利用端末毎の暗号鍵で暗号化して暗号化鍵データを生成し、その生成した暗号化鍵データをマルチキャストで各情報利用端末に配送する。

【００１１】各情報利用端末では、前記マルチキャストで配送された暗号化鍵データを受信して当該情報利用端末内に保存しておき、マルチキャストで配送された暗号化コンテンツを受信した際に、前記情報利用端末内に保存しておいた暗号化鍵データを復号化して鍵を生成し、前記取得した暗号化コンテンツを前記生成した鍵で復号化してコンテンツを利用する。

【００１２】以上の様に本発明の情報配送システムによれば、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するので、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能である。

【００１３】

【発明の実施の形態】以下に暗号化コンテンツを復号化する為の鍵を暗号化した後にマルチキャストで各情報利用端末に配送する一実施形態の情報配送システムについて説明する。

【００１４】図１は本実施形態の情報配送システムの概略構成を示す図である。図１に示す様に本実施形態の情報配送システムは、情報提供端末１と、情報利用端末２～４と、鍵提供端末５とを有している。

【００１５】情報提供端末１は、ストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで情報利用端末２～４に配送する装置である。情報利用端末２～４は、情報提供端末１から配送された暗号化コンテンツをマルチキャストで鍵提供端末５から配送された鍵で復号化して利用する装置である。鍵提供端末５は、暗号化コンテンツを復号化する為の鍵をマルチキャストで情報利用端末２～４に配送する装置である。

【００１６】本実施形態において、情報提供端末１と情報利用端末２～４と鍵提供端末５は、それぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末２～４に配送する情報提供端末１と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末５とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【００１７】図２は本実施形態の情報提供端末１の概略構成を示す図である。図２に示す様に本実施形態の情報提供端末１は、ＣＰＵ２０１と、メモリ２０２と、磁気ディスク装置２０３と、入力装置２０４と、出力装置２０５と、ＣＤ－ＲＯＭ装置２０６と、通信装置２０７とを有している。

【００１８】ＣＰＵ２０１は、情報提供端末１全体の動作を制御する装置である。メモリ２０２は、情報提供端末１全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置２０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００１９】入力装置２０４は、ストリームコンテンツをマルチキャストで各情報利用端末へ配送する為の各種入力を行う装置である。出力装置２０５は、ストリームコンテンツの配送に伴う各種出力を行う装置である。

【００２０】ＣＤ－ＲＯＭ装置２０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置２０７は、インターネットやイントラネット等のネットワークを介して各情報利用端末及び鍵提供端末５との通信を行う装置である。

【００２１】また情報提供端末１は、鍵取得部２１１と、鍵保存部２１２と、コンテンツ暗号化部２１３と、コンテンツ配送部２１４とを有している。

【００２２】鍵取得部２１１は、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末５から取得する処理部である。鍵保存部２１２は、鍵取得部２１１によって取得された鍵をメモリ２０２または磁気ディスク装置２０３に保存する処理部である。

【００２３】コンテンツ暗号化部２１３は、鍵保存部２１２によってメモリ２０２または磁気ディスク装置２０

３に保存された鍵によりコンテンツを暗号化する処理部である。コンテンツ配送部２１４は、コンテンツ暗号化部２１３によって暗号化されたコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送する処理部である。

【００２４】情報提供端末１を鍵取得部２１１、鍵保存部２１２、コンテンツ暗号化部２１３及びコンテンツ配送部２１４として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００２５】図３は本実施形態の情報利用端末２の概略構成を示す図である。図３に示す様に本実施形態の情報利用端末２は、ＣＰＵ３０１と、メモリ３０２と、磁気ディスク装置３０３と、入力装置３０４と、出力装置３０５と、ＣＤ－ＲＯＭ装置３０６と、通信装置３０７とを有している。

【００２６】ＣＰＵ３０１は、情報利用端末２全体の動作を制御する装置である。メモリ３０２は、情報利用端末２全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置３０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００２７】入力装置３０４は、マルチキャストで情報提供端末１から配送されたストリームコンテンツを取得する為の各種入力を行う装置である。出力装置３０５は、ストリームコンテンツの取得に伴う各種出力を行う装置である。

【００２８】ＣＤ－ＲＯＭ装置３０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置３０７は、インターネットやイントラネット等のネットワークを介して情報提供端末１及び鍵提供端末５との通信を行う装置である。

【００２９】また情報利用端末２は、鍵取得部３１１と、鍵保存部３１２と、コンテンツ取得部３１３と、識別情報確認部３１４と、鍵復号化部３１５と、コンテンツ復号化部３１６と、コンテンツ再生部３１７と、鍵変更予告取得部３１８と、鍵確認部３１９と、鍵再配送要求部３２０と、鍵再取得部３２１とを有している。

【００３０】鍵取得部３１１は、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データを鍵提供端末５からマルチキャストで取得する処理部である。鍵保存部３１２は、鍵取得部３１１によって取得された暗号化鍵データをメモリ３０２または磁気ディスク装置３０３に保存する処理部である。

【００３１】コンテンツ取得部３１３は、暗号化コンテンツを情報提供端末１からマルチキャストで取得する処理部である。識別情報確認部３１４は、前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する処理部である。

【００３２】鍵復号化部３１５は、前記保存した暗号化鍵データを復号化して鍵を生成する処理部である。コンテンツ復号化部３１６は、コンテンツ取得部３１３によって取得された暗号化コンテンツを、鍵復号化部３１５で生成した鍵で復号化する処理部である。

【００３３】コンテンツ再生部３１７は、コンテンツ復号化部３１６によって復号化されたコンテンツを再生する処理部である。鍵変更予告取得部３１８は、暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を取得する処理部である。

【００３４】鍵確認部３１９は、前記取得した鍵変更予告で予告された変更後の鍵を取得しているかどうかを確認する処理部である。鍵再配送要求部３２０は、前記変更後の鍵を取得していない場合にその変更後の鍵の再配送を要求する処理部である。鍵再取得部３２１は、前記再配送を要求した変更後の暗号化鍵データを取得する処理部である。

【００３５】情報利用端末２を鍵取得部３１１、鍵保存部３１２、コンテンツ取得部３１３、識別情報確認部３１４、鍵復号化部３１５、コンテンツ復号化部３１６、コンテンツ再生部３１７、鍵変更予告取得部３１８、鍵確認部３１９、鍵再配送要求部３２０及び鍵再取得部３２１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００３６】なお情報利用端末３及び４についても情報利用端末２の構成と同様であるものとする。

【００３７】図４は本実施形態の鍵提供端末５の概略構成を示す図である。図４に示す様に本実施形態の鍵提供端末５は、ＣＰＵ４０１と、メモリ４０２と、磁気ディスク装置４０３と、入力装置４０４と、出力装置４０５と、ＣＤ－ＲＯＭ装置４０６と、通信装置４０７とを有している。

【００３８】ＣＰＵ４０１は、鍵提供端末５全体の動作を制御する装置である。メモリ４０２は、鍵提供端末５全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置４０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００３９】入力装置４０４は、コンテンツを暗号化ま

たは復号化する為の鍵をユニキャストで情報提供端末１及び各情報利用端末へ配送する為の各種入力を行う装置である。出力装置４０５は、コンテンツを暗号化または復号化する為の鍵の配送に伴う各種出力を行う装置である。

【００４０】ＣＤ－ＲＯＭ装置４０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。通信装置４０７は、インターネットやイントラネット等のネットワークを介して情報提供端末１及び各情報利用端末との通信を行う装置である。

【００４１】また鍵提供端末５は、鍵生成部４１１と、鍵暗号化部４１２と、識別情報付加部４１３と、鍵配送部４１４と、鍵更新部４１５と、鍵変更予告配送部４１６と、鍵再配送受付部４１７と、鍵再配送部４１８とを有している。

【００４２】鍵生成部４１１は、コンテンツを暗号化または復号化する為の鍵を生成する処理部である。鍵暗号化部４１２は、前記鍵を暗号化して暗号化鍵データを生成する処理部である。識別情報付加部４１３は、前記生成した鍵及び暗号化鍵データにそれらを識別する為の識別情報を付加する処理部である。

【００４３】鍵配送部４１４は、鍵生成部４１１で生成された鍵を情報提供端末１に配送し、鍵暗号化部４１２で生成された暗号化鍵データをマルチキャストで各情報利用端末に配送する処理部である。鍵更新部４１５は、鍵配送部４１４から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を情報提供端末１に指定する処理部である。

【００４４】鍵変更予告配送部４１６は、暗号化コンテンツの鍵が変更されることを予告する鍵変更予告を各情報利用端末に配送する処理部である。鍵再配送受付部４１７は、変更後の鍵の再配送要求を情報利用端末から受付ける処理部である。鍵再配送部４１８は、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データを再配送する処理部である。

【００４５】鍵提供端末５を鍵生成部４１１、鍵暗号化部４１２、識別情報付加部４１３、鍵配送部４１４、鍵更新部４１５、鍵変更予告配送部４１６、鍵再配送受付部４１７及び鍵再配送部４１８として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００４６】なおコンテンツを暗号化または復号化する為の鍵の生成及び配送を階層化された複数の鍵提供端末５によって行い、処理負荷を分散させても良い。

【００４７】本実施形態の情報提供端末１には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末５から情報提供端末１及び各情報利用端末に鍵を、また情報提供端末１から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末１に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【００４８】図５は本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。図５に示す様に鍵提供端末５は、暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データや鍵の変更を予告する鍵変更予告をマルチキャストで各情報利用端末に配送する処理を行う。

【００４９】図５のステップ５０１で鍵提供端末５の鍵生成部４１１は、所定の時間が経過した場合や情報提供端末１の利用資格者ＤＢ中の利用資格が変更された場合等の暗号鍵Ｋを生成する条件が成立したかどうかを調べ、暗号鍵Ｋを生成する条件が成立した場合にはステップ５０２へ進む。

【００５０】ステップ５０２では、コンテンツＣ（ｉ）を暗号化する為の暗号鍵Ｋを生成する。暗号鍵Ｋとして通信時にＩＰｓｅｃ(IP security protocol)で利用されているものを利用しても構わないものとする。

【００５１】ステップ５０３で鍵暗号化部４１２は、利用資格者ＤＢの内容を参照し、情報提供端末１から配送されるコンテンツＣ（ｉ）の利用資格を持つ利用者について、その情報利用端末ｍの公開鍵Ｐｍを読み出す。ここで、各情報利用端末は公開鍵暗号方式の公開鍵と秘密鍵を生成して公開鍵を鍵提供端末５に送付し、鍵提供端末５は各情報利用端末の公開鍵を保持しているものとする。また利用資格者ＤＢにはどの情報利用端末がコンテンツの利用を許可されているかを示すデータが保持されているものとし、このデータはある間隔で更新されるものとする。

【００５２】ステップ５０４では、前記読み出した情報利用端末ｍの公開鍵Ｐｍを用いて暗号鍵Ｋを暗号化し、暗号化鍵データＰｍ（Ｋ）を生成する。ここで暗号鍵Ｋの暗号化の際に暗号鍵Ｋのスクランブル処理やハッシュ処理を併用しても良い。

【００５３】ステップ５０５では、前記利用資格を持つ全ての利用者の情報利用端末について、その公開鍵Ｐ１、Ｐ２、．．．Ｐｍ、．．．Ｐｎ（１≦ｍ≦ｎ）を用

いて暗号化鍵データＰ１（Ｋ）、Ｐ２（Ｋ）、．．．Ｐｍ（Ｋ）、．．．Ｐｎ（Ｋ）の生成を行ったかどうかを調べ、利用資格者ＤＢ中にまだ処理を行っていないレコードがある場合にはステップ５０３へ戻って暗号化鍵データの生成を続行し、利用資格を持つ全ての利用者の情報利用端末への暗号化鍵データの生成を完了した場合にはステップ５０６へ進む。

【００５４】ステップ５０６で識別情報付加部４１３は、前記生成された暗号鍵Ｋ及び暗号化鍵データＰ１（Ｋ）、Ｐ２（Ｋ）、．．．Ｐｍ（Ｋ）、．．．Ｐｎ（Ｋ）に識別情報ｉを付加して鍵配送部４１４へ渡す。この識別情報はＩＰｓｅｃのＳＡ(Security Association)に含まれる情報を利用しても構わないものとする。

【００５５】ステップ５０７で鍵配送部４１４は、前記生成された暗号鍵Ｋ（ｉ）をユニキャストで情報提供端末１へ配送すると共に、前記生成された暗号化鍵データＰ１（Ｋ（ｉ））、Ｐ２（Ｋ（ｉ））、．．．Ｐｍ（Ｋ（ｉ））、．．．Ｐｎ（Ｋ（ｉ））をマルチキャストで各情報利用端末へ配送する。ここで前記生成された全暗号化鍵データをある数毎に分割して送信しても良い。

【００５６】ステップ５０８で鍵変更予告配送部４１６は、現在使われている暗号鍵Ｋ（ｉ－１）が暗号鍵Ｋ（ｉ）に変更されることを予告する鍵変更予告Ｙ（ｉ）をマルチキャストで各情報利用端末に配送する。

【００５７】ステップ５０９で鍵再配送受付部４１７は、変更後の暗号鍵Ｋ（ｉ）の再配送要求を情報利用端末から受信しているかどうかを調べ、変更後の暗号鍵Ｋ（ｉ）の再配送要求を受信している場合にはステップ５１０へ進む。

【００５８】ステップ５１０では、利用資格者ＤＢの内容を参照し、前記変更後の暗号鍵Ｋ（ｉ）の再配送要求が、利用資格を持つ利用者の情報利用端末から送信されていることを確認した後、その情報利用端末の公開鍵Ｐｍを読み出して暗号化鍵データＰｍ（Ｋ（ｉ））を再生成する。

【００５９】ステップ５１１で鍵再配送部４１８は、前記再配送要求を行った情報利用端末に変更後の暗号化鍵データＰｍ（Ｋ（ｉ））を再配送する。この際、マルチキャストで再配送を行っても良いし、ユニキャストで直接情報利用端末ｍに配送しても構わないものとする。

【００６０】ステップ５１２では、利用資格を持った全ての利用者に対する暗号鍵Ｋ（ｉ）の配送が完了したことを示す鍵配送完了通知を鍵更新部４１５に伝え、ステップ５１３で鍵更新部４１５は、配送が完了した暗号鍵Ｋ（ｉ）を次の暗号化処理で使用する鍵として決定し、その暗号鍵Ｋ（ｉ）の識別情報ｉ或いは暗号鍵Ｋ（ｉ）そのものの情報を情報提供端末１のコンテンツ暗号化部２１３に通知してステップ５０１へ戻る。

【００６１】前記の様に本実施形態の情報配送システムでは、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送しているので、複数の情報利用端末への鍵の配送を効率的に行うことが可能である。

【００６２】図６は本実施形態の各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図６に示す様に各情報利用端末は、暗号化コンテンツを復号化する為の鍵を暗号化した暗号化鍵データを鍵提供端末５からマルチキャストで取得する処理を行う。また鍵変更予告で予告された変更後の鍵を取得していない場合にはその変更後の鍵の再配送を要求する処理を行う。

【００６３】図６のステップ６０１で情報利用端末ｍの鍵取得部３１１は、鍵提供端末５からマルチキャストで暗号化鍵データＰ１（Ｋ（ｉ））、Ｐ２（Ｋ（ｉ））、．．．Ｐｍ（Ｋ（ｉ））、．．．Ｐｎ（Ｋ（ｉ））を受信しているかどうかを調べ、暗号化鍵データを受信している場合にはステップ６０２へ進み、前記受信した暗号化鍵データの中からその情報利用端末ｍの公開鍵Ｐｍで暗号化された暗号化鍵データＰｍ（Ｋ（ｉ））を取得して鍵保存部３１２に渡す。

【００６４】ステップ６０３で鍵保存部３１２は、鍵提供端末５の識別情報付加部４１３によって付加された識別情報ｉを暗号化鍵データＰｍ（Ｋ（ｉ））から読み出し、ステップ６０４では、ステップ６０２で取得した暗号化鍵データＰｍ（Ｋ（ｉ））をステップ６０３で読み出した識別情報ｉ毎に分類してメモリ３０２または磁気ディスク装置３０３に保存する。ここで各情報利用端末が暗号鍵Ｋ（ｉ）を磁気ディスク装置３０３に保存する場合には暗号化鍵データＰｍ（Ｋ（ｉ））を復号化した暗号鍵Ｋ（ｉ）を保存することとしても良い。

【００６５】ステップ６０５で鍵変更予告取得部３１８は、現在使われている暗号鍵Ｋ（ｉ－１）が暗号鍵Ｋ（ｉ）に変更されることを予告する鍵変更予告Ｙ（ｉ）を鍵提供端末５から受信しているかどうかを調べ、鍵変更予告Ｙ（ｉ）を受信している場合にはステップ６０６へ進む。

【００６６】ステップ６０６で鍵確認部３１９は、前記取得した鍵変更予告Ｙ（ｉ）で予告された変更後の暗号鍵Ｋ（ｉ）を取得しているかどうかを調べ、鍵変更予告Ｙ（ｉ）に示された識別情報ｉの暗号化鍵データＰｍ（Ｋ（ｉ））がメモリ３０２または磁気ディスク装置３０３に保存されていない場合にはステップ６０７へ進む。

【００６７】ステップ６０７で鍵再配送要求部３２０は、前記変更後の暗号鍵Ｋ（ｉ）の再配送を鍵提供端末５に要求する。ステップ６０８で鍵再取得部３２１は、前記再配送を要求した変更後の暗号化鍵データＰｍ（Ｋ（ｉ））を鍵提供端末５から受信してメモリ３０２または磁気ディスク装置３０３に保存する。

【００６８】前記の様に本実施形態の情報配送システムでは、暗号化コンテンツの鍵が変更されることを予告す

る鍵変更予告を鍵提供端末５から各情報利用端末に送信し、鍵の再配送を行っているので、暗号化コンテンツを復号化する為の鍵が、マルチキャストの際の通信パケットの欠落や通信の遅延で送付されなかった場合に鍵を再配送し、正当な利用者が確実にストリームコンテンツを利用できる様にしている。

【００６９】図７は本実施形態の情報提供端末１のコンテンツ配送処理の処理手順を示すフローチャートである。図７に示す様に情報提供端末１のコンテンツ暗号化部２１３は、鍵取得部２１１により鍵提供端末５から取得し鍵保存部２１２によって保存された鍵の内、鍵提供端末５の鍵更新部４１５により指定された識別情報ｉの暗号鍵Ｋ（ｉ）を用いてコンテンツＣ（ｉ）を暗号化し、前記暗号化されたコンテンツである暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））をコンテンツ配送部２１４によりマルチキャストで各情報利用端末に配送する処理を行う。

【００７０】図７のステップ７０１で情報提供端末１のコンテンツ暗号化部２１３は、鍵保存部２１２によってメモリ２０２または磁気ディスク装置２０３に保存されていた鍵の内、鍵提供端末５の鍵更新部４１５により指定された識別情報ｉの暗号鍵Ｋ（ｉ）を読み出す。

【００７１】ステップ７０２では、配送対象のコンテンツＣ（ｉ）を所定の単位で読み出し、ステップ７０３では、ステップ７０２で読み出したコンテンツＣ（ｉ）のデータをステップ７０１で読み出した暗号鍵Ｋ（ｉ）で暗号化して暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））を生成し、コンテンツ配送部２１４に渡す。ここで暗号化の単位はネットワーク配送を行う為のパケットの大きさを単位としても構わないものとする。またコンテンツの暗号化の際にコンテンツのスクランブル処理やハッシュ処理を併用しても良い。

【００７２】ステップ７０４でコンテンツ配送部２１４は、前記生成された暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））のヘッダー等に暗号鍵Ｋ（ｉ）の識別情報ｉを付加する。なおここでＩＰｓｅｃのヘッダーを利用しても構わないものとする。

【００７３】ステップ７０５では、前記識別情報ｉの付加された暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））をマルチキャストで情報利用端末２～４へ配送する。ステップ７０６では、配送対象のコンテンツＣ（ｉ）について全てのデータを情報利用端末２～４に配送したかどうかを調べ、まだ配送を行っていないデータがある場合にはステップ７０２へ戻ってコンテンツＣ（ｉ）の配送を続行し、全データの配送を完了した場合にはコンテンツＣ（ｉ）の配送処理を終了する。

【００７４】図８は本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。図８に示す様に各情報利用端末は、マルチキャストで配送された暗号化鍵データを復号化して生成した鍵を用いて暗号化コンテンツを復号化する処理を行う。

【００７５】図８のステップ８０１で各情報利用端末のコンテンツ取得部３１３は、情報提供端末１からマルチキャストで暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））を受信しているかどうかを調べ、暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））を受信している場合にはステップ８０２へ進み、前記受信した暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））を取得して識別情報確認部３１４に渡す。

【００７６】ステップ８０３で識別情報確認部３１４は、前記取得した暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））のヘッダー等を参照し、暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））に付加されている識別番号ｉを確認して鍵復号化部３１５へ通知する。

【００７７】ステップ８０４で鍵復号化部３１５は、識別情報確認部３１４から通知されたものと同一の識別番号ｉを持つ暗号鍵Ｋ（ｉ）の読込みが未実行であるかどうかを調べ、暗号鍵Ｋ（ｉ）の読込みが未実行である場合にはステップ８０５へ進む。

【００７８】ステップ８０５では、鍵保存部３１２によってメモリ３０２または磁気ディスク装置３０３に保存されている暗号化鍵データの内、識別情報確認部３１４から通知されたものと同一の識別番号ｉを持つ暗号化鍵データＰｍ（Ｋ（ｉ））を読み出す。ステップ８０６では、前記読み出した暗号化鍵データＰｍ（Ｋ（ｉ））を情報利用端末ｍの公開鍵Ｐｍに対応する秘密鍵で復号化し、暗号鍵Ｋ（ｉ）を生成する。

【００７９】ステップ８０７でコンテンツ復号化部３１６は、ステップ８０２で取得した暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））をステップ８０６で生成した暗号鍵Ｋ（ｉ）によって復号化してコンテンツＣ（ｉ）を生成し、ステップ８０７でコンテンツ再生部３１７は、前記復号化によって得られたコンテンツＣ（ｉ）を再生してステップ８０１へ戻る。

【００８０】前記の様に本実施形態では、情報提供端末１から配送されるコンテンツＣ（ｉ）の利用資格を持つ利用者の情報利用端末へマルチキャストで暗号化鍵データＰｍ（Ｋ（ｉ））（復号兼用）を配送した後、暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツ及び鍵の提供を行うことができる。

【００８１】また前記の例では、暗号化鍵データ、鍵変更予告Ｙ、暗号化コンテンツを別々に配送しているが、それらの２つ以上を同一のパケットに合成してマルチキャストで配送を行しても良い。

【００８２】すなわちステップ５０７で鍵提供端末５の鍵配送部４１４は、前記生成された暗号鍵Ｋ（ｉ）と共に暗号化鍵データＰ１（Ｋ（ｉ））、Ｐ２（Ｋ（ｉ））、．．．Ｐｍ（Ｋ（ｉ））、．．．Ｐｎ（Ｋ

（ｉ））をユニキャストで情報提供端末１へ配送する。

【００８３】またステップ５０８で鍵変更予告配送部４１６は、暗号化コンテンツの暗号鍵Ｋ（ｉ－１）が暗号鍵Ｋ（ｉ）に変更されることを予告する鍵変更予告Ｙ（ｉ）をユニキャストで情報提供端末１へ配送する。

【００８４】そしてステップ７０４で情報提供端末１のコンテンツ配送部２１４は、単数または複数の暗号化鍵データ（例えばＰ１（Ｋ（ｉ））とＰ２（Ｋ（ｉ））等）や、暗号鍵Ｋ（ｉ－１）が暗号鍵Ｋ（ｉ）に変更されることを予告する鍵変更予告Ｙ（ｉ）を暗号化コンテンツＫ（ｉ－１）（Ｃ（ｉ－１））の一部と同一のパケットに合成し、ステップ７０５でマルチキャストにより各情報利用端末へ配送する。ここで暗号化コンテンツＫ（ｉ－１）（Ｃ（ｉ－１））は、暗号鍵Ｋ（ｉ）の前に生成された暗号鍵Ｋ（ｉ－１）によってコンテンツＣ（ｉ－１）を暗号化したものである。

【００８５】各情報利用端末では、暗号化鍵データＰ１（Ｋ（ｉ））、Ｐ２（Ｋ（ｉ））、．．．Ｐｍ（Ｋ（ｉ））、．．．Ｐｎ（Ｋ（ｉ））、鍵変更予告Ｙ（ｉ）、暗号化コンテンツＫ（ｉ－１）（Ｃ（ｉ－１））の内の２つ以上のデータを同一のマルチキャストにより取得し、各取得部によりそれら分離して取得する。

【００８６】この様に暗号化コンテンツＫ（ｉ－１）（Ｃ（ｉ－１））と、変更後の暗号鍵Ｋ（ｉ）の暗号化鍵データＰ１（Ｋ（ｉ））、Ｐ２（Ｋ（ｉ））、．．．Ｐｍ（Ｋ（ｉ））、．．．Ｐｎ（Ｋ（ｉ））や、暗号鍵Ｋ（ｉ－１）が暗号鍵Ｋ（ｉ）に変更されることを予告する鍵変更予告Ｙ（ｉ）を同一のマルチキャストで配送することにより、コンテンツを利用している各情報利用端末に、より確実に変更後の暗号鍵Ｋ（ｉ）を配送することができる。

【００８７】また前記の例では、暗号化コンテンツを復号化する為の鍵を各情報利用端末の公開鍵で暗号化して暗号化鍵データを生成しているが、各情報利用端末と鍵提供端末５とが共有する共通秘密鍵を用いて暗号化鍵データを生成しても良い。

【００８８】すなわちステップ５０３～ステップ５０５で鍵提供端末５の鍵暗号化部４１２は、利用資格者ＤＢの内容を参照し、情報提供端末１から配送されるコンテンツＣ（ｉ）の利用資格を持つ利用者について、その情報利用端末の共通秘密鍵Ｓ１、Ｓ２、．．．Ｓｍ、．．．Ｓｎ（１≦ｍ≦ｎ）を用いて暗号化鍵データＳ１（Ｋ）、Ｓ２（Ｋ）、．．．Ｓｍ（Ｋ）、．．．Ｓｎ（Ｋ）を生成する。ここで、各情報利用端末は情報利用端末または利用者の個別情報を利用して共通秘密鍵を生成して鍵提供端末５に送付しているものとする。なお前記個別情報とは、各情報利用端末が生成していた秘密鍵、媒体固有番号、ＩＰアドレス、利用者のユーザＩＤ、パスワード、生年月日等のユーザ個人情報である。

【００８９】そしてステップ８０６では、暗号化鍵データＳｍ（Ｋ（ｉ））を情報利用端末ｍの共通秘密鍵Ｓｍで復号化して暗号鍵Ｋ（ｉ）を生成し、暗号化コンテンツＫ（ｉ）（Ｃ（ｉ））の復号化に用いる。

【００９０】以上説明した様に本実施形態の情報配送システムによれば、暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するので、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能である。

【００９１】また本実施形態の情報配送システムによれば、暗号化コンテンツの鍵が変更されることを予告し、要求に応じて鍵の再配送を行なうので、暗号化コンテンツを復号化する為の鍵の配送をより確実に行うことが可能である。

【００９２】

【発明の効果】本発明によれば暗号化コンテンツを復号化する為の鍵をマルチキャストで各情報利用端末に配送するので、暗号化コンテンツを復号化する為の鍵を複数の情報利用端末に効率良く配送することが可能である。

【図面の簡単な説明】

【図１】本実施形態の情報配送システムの概略構成を示す図である。

【図２】本実施形態の情報提供端末１の概略構成を示す図である。

【図３】本実施形態の情報利用端末２の概略構成を示す図である。

【図４】本実施形態の鍵提供端末５の概略構成を示す図である。

【図５】本実施形態の鍵提供端末５の鍵配送処理の処理手順を示すフローチャートである。

【図６】本実施形態の各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図７】本実施形態の情報提供端末１のコンテンツ配送処理の処理手順を示すフローチャートである。

【図８】本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。

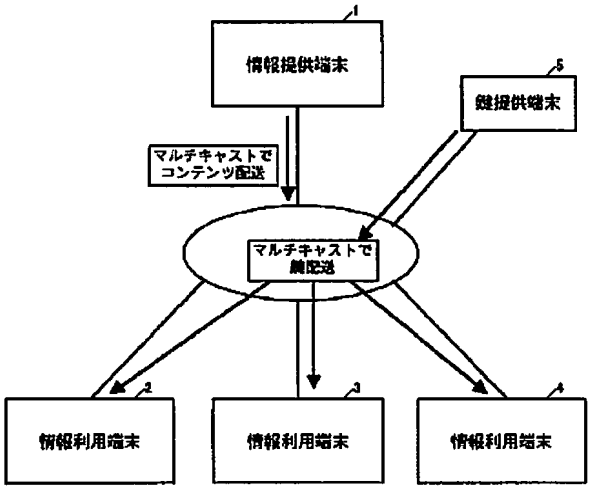
【符号の説明】

１…情報提供端末、２～４…情報利用端末、５…鍵提供端末、２０１…ＣＰＵ、２０２…メモリ、２０３…磁気ディスク装置、２０４…入力装置、２０５…出力装置、２０６…ＣＤ－ＲＯＭ装置、２０７…通信装置、２１１…鍵取得部、２１２…鍵保存部、２１３…コンテンツ暗号化部、２１４…コンテンツ配送部、３０１…ＣＰＵ、３０２…メモリ、３０３…磁気ディスク装置、３０４…入力装置、３０５…出力装置、３０６…ＣＤ－ＲＯＭ装置、３０７…通信装置、３１１…鍵取得部、３１２…鍵保存部、３１３…コンテンツ取得部、３１４…識別情報確認部、３１５…鍵復号化部、３１６…コンテンツ復号化部、３１７…コンテンツ再生部、３１８…鍵変更予告取得部、３１９…鍵確認部、３２０…鍵再配送要求部、

３２１…鍵再取得部、４０１…ＣＰＵ、４０２…メモリ、４０３…磁気ディスク装置、４０４…入力装置、４０５…出力装置、４０６…ＣＤ－ＲＯＭ装置、４０７…通信装置、４１１…鍵生成部、４１２…鍵暗号化部、４１３…識別情報付加部、４１４…鍵配送部、４１５…鍵更新部、４１６…鍵変更予告配送部、４１７…鍵再配送受付部、４１８…鍵再配送部。

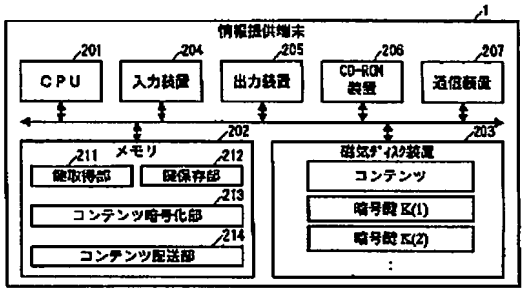
【図１】

図１



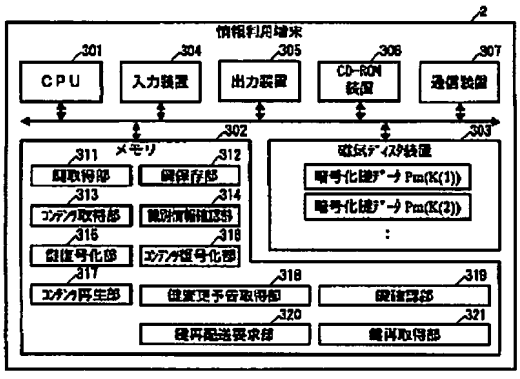
【図２】

図２



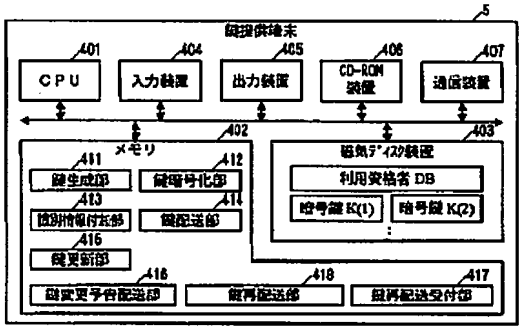
【図３】

図３



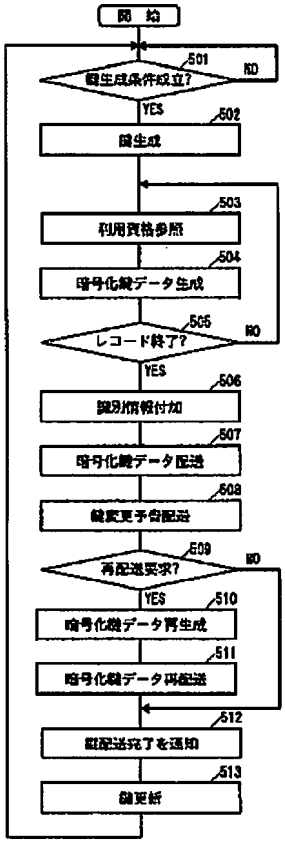
【図４】

図４



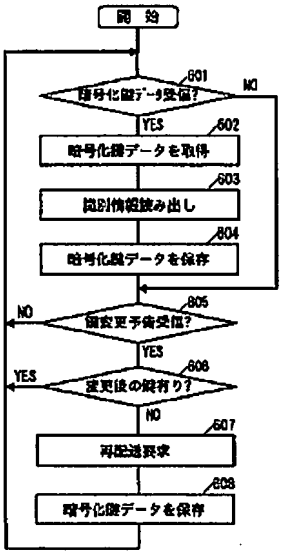
【図５】

図５



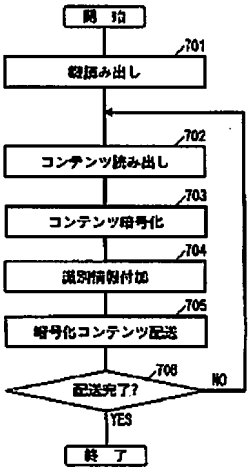
【図６】

図６



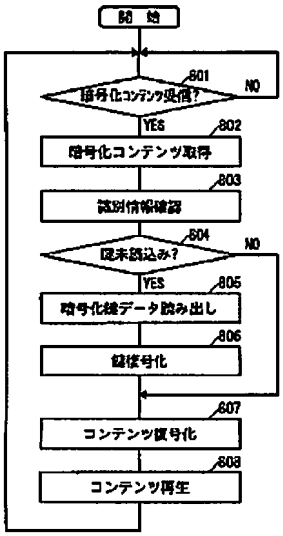
【図７】

図７



【図８】

図８



フロントページの続き

(72)発明者　中里　加奈
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA01 AA16 BA03 EA01 EA04 EA17 NA02 PA04 PA05